Manual enrollment.

Using this method, the private key and a certificate request are generated on a device, such as a Web service or a computer. The certificate request is then transported to the CA to generate the certificate being requested. The certificate is then transported back to the device for installation. Use this method when the requestor cannot communicate directly with the CA, or if the device does not support autoenrollment.

CA Web enrollment.

Using this method, you can enable a website CA so that users can obtain certificates. To use CA Web enrollment, you must install Internet Information Server (IIS) and the web enrollment role on the CA of AD CS. To obtain a certificate, the requestor logs on to the website, selects the appropriate certificate template, and then submits a request. The certificate is issued automatically if the user has the appropriate permissions to enroll for the certificate. The CA Web enrollment method should be used to issue certificates when autoenrollment cannot be used. This can happen in the case of an Advanced Certificate request. However, there are cases where autoenrollment can be used for certain certificates, but not for all certificates.

Enrollment on behalf (Enrollment Agent).

Using this method, a CA administrator creates an Enrollment Agent account for a user. The user with Enrollment Agent rights can then enroll for certificates on behalf of other users. You would use this method, for example, if you need to allow a manager to preload logon certificates of new employees on to smart cards

The **restricted Enrollment Agent** is a functionality that was introduced in the Windows Server 2008 Enterprise operating system. This functionality allows you to limit the permissions for users who are designated as Enrollment Agents, to enroll for smart card certificates on behalf of other users.

Typically, one or more authorized individuals within an organization are designated as Enrollment Agents. The Enrollment Agent needs to be issued an Enrollment Agent

certificate, which enables the agent to enroll for smart card certificates on behalf of users. Enrollment agents are typically members of corporate security, IT security, or help desk teams, because these individuals have already been entrusted with safeguarding valuable resources.

On a Windows Server 2012 CA, the restricted Enrollment Agent features allow an Enrollment Agent to be used for one or many certificate templates. For each certificate template, you can choose on behalf of which users or security groups the Enrollment Agent can enroll. You cannot constrain an Enrollment Agent based on a certain Active Directory organizational unit (OU) or container; instead, you must use security groups.

Note: Using restricted Enrollment Agents will affect the performance of the CA. To optimize performance, you should minimize the number of accounts that are listed as Enrollment Agents. You minimize the number of accounts in the Enrollment Agent's permissions list. As a best practice, use group accounts in both lists instead of individual user accounts.